Quantum Communication between N-partners and Bell's Inequalities

Valerio Scarani*, Nicolas Gisin

Group of Applied Physics, University of Geneva
20, rue de l'Ecole-de-Médecine, CH-1211 Geneva 4, Switzerland

We consider a family of quantum communication protocols involving N partners. We demonstrate the existence of a link between the security of these protocols against individual attacks by the eavesdropper, and the violation of some Bell's inequalities, generalizing the link that was noticed some years ago for two-partners quantum cryptography. The arguments are independent of the local hidden variable debate.

Historically, entanglement was essentially a source of controversy on the foundations of quantum mechanics, as illustrated by the lively debate about the local hidden variable program and Bell's inequality [1]. Today, it is widely recognized that entanglement is a resource from which tasks can be achieved that are classically impossible, as illustrated by many quantum information protocols [2]. Among these protocols, quantum cryptography — better described as quantum key distribution (QKD) — is the one that has almost reached the level of application [3]. In this work, we study the link between the security of quantum communication protocols and the violation of Bell's inequalities. Previous works [4,5] pointed out such a link in QKD between two partners Alice and Bob. We begin by reviewing these results, that will help to clarify the initial intuition and the motivation for the present work.

Consider the following QKD setup [6]. Alice prepares an EPR state, say $|\Phi_z^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where we write $|0\rangle$ and $|1\rangle$ for the eigenstates of σ_z. She keeps one qubit and sends the other one to Bob. Alice and Bob measure either σ_x or σ_y, then publicly communicate the choice of the measurement basis. Whenever they have used the same basis, their results are perfectly correlated, and they can establish a key. This protocol is equivalent to the BB84 protocol [7]. Its distinguishing feature is the fact that the bits are encoded into orthogonal states belonging to two conjugated bases.

To study the security of the protocol, consider an eavesdropper (Eve) that acts on the quantum channel linking Alice to Bob, trying to get some information but inevitably introducing perturbations. To establish a key in spite of these perturbations, A and B can run a one-way protocol called *error correction and privacy amplification* if and only if [8]

$$I(A:B) > \min[I(A:E), I(B:E)] \qquad (1)$$

where $I(A:B) = H(A) + H(B) - H(AB)$, H the Shannon entropy, is called *mutual information*. In the following, we shall consider (1) as the condition for security, although it is known that a secret key can be established under less restrictive conditions by using two-way communication [9].

In our context, Eve's best attack is defined as the attack that maximizes $I(A:E)$ for a fixed $I(A:B)$. The best attack is not known in all generality [10]; but it is, if we suppose that Eve performs an *individual attack*, that is, that she makes only measurements on individual qubits [5]. Moreover, it is also known that Eve can perform the best individual attack by using a single qubit as resource [11], by implementing the following unitary transformation affecting her and Bob's qubits:

$$\begin{aligned} U_{BE}|00\rangle &= |00\rangle \\ U_{BE}|10\rangle &= \cos\phi|10\rangle + \sin\phi|01\rangle \end{aligned} \qquad (2)$$

Here, $|00\rangle$ etc. are shorthand for $|0\rangle_B \otimes |0\rangle_E$ etc. (by convention, we supposed that Eve prepares her qubits in the state $|0\rangle$), and $\phi \in [0, \frac{\pi}{2}]$ characterizes the strength of Eve's attack. Thus, after eavesdropping the system of three qubits is in the state $|\Psi_{ABE}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes U_{BE}|00\rangle + |1\rangle_A \otimes U_{BE}|10\rangle)$. Note that the roles of B and E are symmetric under the exchange of ϕ with $\frac{\pi}{2} - \phi$. The mutual information between any two partners can be calculated explicitly [12]: condition (1) for security is fulfilled if and only if $\phi < \frac{\pi}{4}$.

As we said above, there is a remarkable link between the security of the BB84 protocol against individual attacks and the violation of Bell's inequalities. For any set of four unit vectors $\underline{a} = \{\vec{a}_1, \vec{a}'_1, \vec{a}_2, \vec{a}'_2\}$, let's define the two-qubit Bell operator

$$B_2(\underline{a}) = (\sigma_{a_1} + \sigma_{a'_1}) \otimes \sigma_{a_2} + (\sigma_{a_1} - \sigma_{a'_1}) \otimes \sigma_{a'_2} \qquad (3)$$

with $\sigma_a = \vec{a} \cdot \vec{\sigma}$. The CHSH inequality [13] reads $S_2 = \max_{\underline{a}} \mathrm{Tr}(\rho\, B_2(\underline{a})) \leq 2$, while the maximal value allowed by QM is $S_2 = 2\sqrt{2}$ [14]. The CHSH inequality is optimal, in the sense it is violated if and only if the statistics of the results cannot be accounted for by local hidden variables (lhv) [15]. The Horodecki criterion [16] allows an explicit calculation of S for each two-qubit state obtained from $|\Psi_{ABE}\rangle$ by tracing out the third qubit. We find that the pair B-E never violates the inequality, while

$$S_{AB} = 2\sqrt{2}\cos\phi \,, \quad S_{AE} = 2\sqrt{2}\sin\phi \,. \qquad (4)$$

Then obviously $S_{AB} > 2$ if and only if $S_{AE} < 2$: the inequality is violated by the pair A-B if and only if it

*valerio.scarani@physics.unige.ch

is not violated by the pair A-E. In conclusion, for the QKD protocol that we consider, (1) holds if and only if $S_{AB} > 2 > S_{AE}$ (fig. 1).
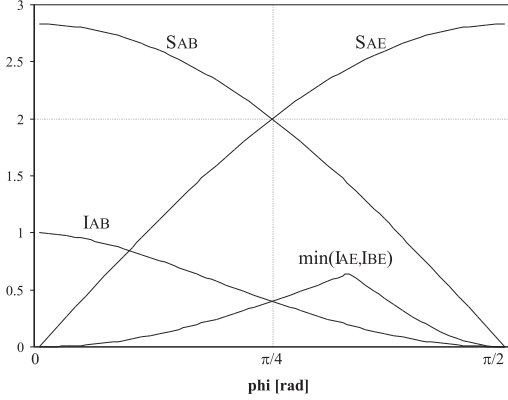

FIG. 1. The link between violation of Bell's inequality and the security condition (1), in the case of the two-partners QKD with best individual attack by Eve.

The previous paragraphs summarize the present knowledge about the link between security and Bell's inequalities. In the following, we shall generalize this link for QKD protocols involving an arbitrary number of partners. But before turning to this, let's address the following purely algebraic problem, which is naturally related to this discussion. Consider three partners A, B and C (here there is no more reason to single out an Eve), each possessing a qubit. Are there pure or mixed states of the three qubit system such that more than one pair can violate the CHSH inequality? The answer to this question is negative:

Theorem 1: *Let ρ be a three-qubit state, and ρ_{AB}, ρ_{BC} and ρ_{AC} be the two-qubit states obtained from ρ by tracing out one of the qubits. If one can find four unit vectors $\vec{a}, \vec{a}', \vec{b}, \vec{b}'$ such that $Tr(B_2 \rho_{AB}) > 2$, then for all choice of four unit vectors $Tr(B_2 \rho_{BC}) < 2$ and $Tr(B_2 \rho_{AC}) < 2$.* We present a proof inspired by Cirel'son's proof that the maximal violation of CHSH allowed by quantum mechanics is $2\sqrt{2}$ [14]. Let's define the operator

$$ V = B_{AB}(\vec{a}, \vec{a}', \vec{b}, \vec{b}') + B_{AC}(\vec{A}, \vec{A}', \vec{c}, \vec{c}'). \qquad (5) $$

where $B_{AB} = B_2 \otimes \mathbb{1}_C$, and similarly for B_{AC}. Using $\sigma_a \sigma_{a'} = (\vec{a} \cdot \vec{a}')\mathbb{1} + i\sigma_{a \wedge a'}$, lengthy but standard algebra leads to $\left(\frac{V^2}{4} - 2\mathbb{1}\right)^2 = f\mathbb{1}$, where f is a function of the unit vectors that satisfies $0 \leq f \leq 4$ [17]. This entails $|\langle V \rangle_\rho| \leq 4$, that is $\max |\langle B_{AB} + B_{AC} \rangle_\rho| \leq 4$, where the maximum is taken over the eight unit vectors that define V. But due to the symmetry $B_{AB}(\vec{a}, \vec{a}', -\vec{b}, -\vec{b}') = -B_{AB}(\vec{a}, \vec{a}', \vec{b}, \vec{b}')$, it holds that $\max |\langle B_{AB} + B_{AC} \rangle_\rho| = \max |\langle B_{AB} \rangle_\rho| + \max |\langle B_{AC} \rangle_\rho| = S_{AB} + S_{AC}$. In conclusion, $S_{AB} + S_{AC} \leq 4$ for all ρ and for all choice of unit vectors. This proves the theorem.

Two remarks: (i) It is easy to imagine experimental protocols in which, for suitable states, both pairs A-B and A-C end up with a violation of the inequality: e.g., a pair can analyze their data conditioning on the results of the third partner, if they know this result through classical communication; or, a pair may apply a filtering procedure [18]. (ii) There are states depending on one or more parameters such that one can "shift" the violation from one pair to another by varying the parameters: the state introduced above in the context of QKD, in particular, is such that $S_{AB}(\phi) > 2$ if and only if $S_{AC}(\phi) < 2$ [19].

We explore now the generalization of the link between Bell's inequalities and security to QKD protocols involving more than two partners. The protocols that we consider are characterized by the fact that the sender distributes the key between several partners, in such a way that *all partners must collaborate* to retrieve the key. We call these protocols *N-partners quantum secret sharing* (N-QSS) [20]. For simplicity, we discuss in detail the protocol 3-QSS involving three partners, and discuss later how this generalizes to an arbitrary number of partners. Without eavesdropping, 3-QSS works as follows. Alice prepares the 3-qubit GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$; she keeps one qubit and sends the others to her two partners Bob and Charlie. The three of them measure σ_x or σ_y; the GHZ state is such that $\langle \sigma_x \otimes \sigma_x \otimes \sigma_x \rangle = -\langle \sigma_x \otimes \sigma_y \otimes \sigma_y \rangle = -\langle \sigma_y \otimes \sigma_x \otimes \sigma_y \rangle = -\langle \sigma_y \otimes \sigma_y \otimes \sigma_x \rangle = 1$, and the other expectation values vanish. Then A, B and C publicly announce the bases they used, and keep only those measurements when all measured σ_x, or when one measured σ_x and the others σ_y. It is easy to see that each partner alone has no information on the key of any other partner, but if two partners collaborate then they have all the information about the key of the third partner. Therefore the meaningful information measure is the information that B and C together have on A's sequence of bits, that is $I(A : BC) = H(A) - H(A|BC) = 1 - H(A|BC)$. In the absence of eavesdropping, $H(A|BC) = 0$.

Two eavesdropping scenarios can be imagined:

Scenario 1: An external Eve tries to eavesdrop on both channels A-B and A-C. We still restrict to attacks that are "individual" in the sense that each pair of qubits is attacked independently from all the other pairs; but we allow coherent measurements on the two qubits of each pair.

Scenario 2: Charlie is dishonest: he would like to retrieve the key alone, against the will of Alice who would force him and Bob to collaborate. Then C collaborates with Eve, who tries to eavesdrop on the line A-B in order to get as much as possible information about Bob's qubit.

The security issue on these protocols is analogous to the two partners case. We sketch the argument, see [12] for all details. The key of the demonstration is the fact that the time ordering of the measurements is not important: if (say) the time of Alice's measurement would

change something in the local statistics of her partners or in their correlations, the protocol would allow signaling. Therefore, we can discuss security on completely equivalent protocols in which some partners measure their qubits first, this measurement acting as a preparation on the state of the other qubits.

Take Scenario 1 first: When Alice measures her qubit, she prepares one of the four states $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $\frac{1}{\sqrt{2}}(|00\rangle \pm i|11\rangle)$. Therefore, one can see this protocol as a two-partners communication, Alice sending information to Bob-Charlie. Since we want to maximize $I(A:E)$ for a fixed $I(A:BC)$, Eve's best individual attack can be copied directly from (2), replacing $|0\rangle_B$ and $|1\rangle_B$ by $|00\rangle_{BC}$ and $|11\rangle_{BC}$ respectively:

$$\begin{aligned} U_{BCE}|000\rangle &= |000\rangle \\ U_{BCE}|110\rangle &= \cos\phi|110\rangle + \sin\phi|001\rangle \end{aligned} \quad (6)$$

In particular, Eve can still perform the best individual attack by using a single qubit. This is surprisingly simple, because a priori Eve needs an increasing number of qubits (2^{2n}) to perform the most general attack on n qubits. However, even if Eve does not need a larger probe, she must be able to implement a coherent operation on a bigger number of qubits. Under this respect, eavesdropping on several channels is more complicated than on a single channel.

Scenario 2 can be discussed in the same way: When A and C measure their qubit, we have a single qubit flying to B, encoded as in the BB84 protocol, and on which E eavesdrops. We just have to be careful because the direct analogy with the two-partners case gives us the optimum of $I(A:E)$ for a given value of $I(AC:B)$, not of $I(A:BC)$. However, by the very definition of the protocol, B and C are not correlated, whence $I(AC:B) = I(A:BC)$. Therefore, in Scenario 2 Eve's best individual attack on Bob's qubit is (2).

The same arguments can be worked out for the protocol N-QSS involving N partners. The general eavesdropping scenario is shown in fig. 2: $n < N-1$ partners (Charlies, $\underline{C}$) are dishonest, and want to retrieve the key without the help of the $N-1-n \equiv h$ other partners (Bobs, $\underline{B}$). Then again Eve can perform the best individual attack using a single qubit, which must interact coherently with all the h qubits that are to be spied. The state of the $N+1$ qubits after eavesdropping is

$$\begin{aligned} |\Psi_{Nh}\rangle = \frac{1}{\sqrt{2}} \big(&|0^{N-h}\rangle|0^h\rangle|0\rangle + \cos\phi|1^{N-h}\rangle|1^h\rangle|0\rangle \\ &+ \sin\phi|1^{N-h}\rangle|0^h\rangle|1\rangle \big) \end{aligned} \quad (7)$$

where the first ket are A and the dishonest $\underline{C}$, the second ket are the honest $\underline{B}$ that are spied, the third ket is Eve. Let $I_a = I(A:\underline{BC})$ the information between the authorized partners, $I_u = I(A:\underline{C}E)$ the information between the unauthorized partners. In analogy with the case of two partners QKD, it can be shown that $I_a > I_u$ if and only if $\phi < \frac{\pi}{4}$ [12]. Now we can tackle the link with Bell's inequalities.
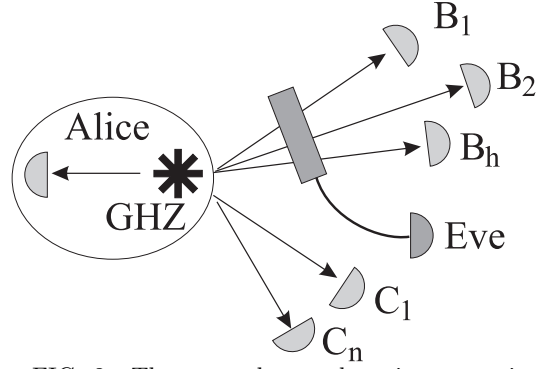

FIG. 2. The general eavesdropping scenario on N-QSS, with h honest Bobs and $n = N - h - 1$ dishonest Charlies collaborating with Eve.

For our study, we consider the family of inequalities known as Mermin-Klyshko (MK) inequalities [21,22]. This choice will be discussed below. The Bell operator for M qubits is defined recursively as

$$B_M = \frac{\sigma_{a_M} + \sigma_{a'_M}}{2} \otimes B_{M-1} + \frac{\sigma_{a_M} - \sigma_{a'_M}}{2} \otimes B'_{M-1} \quad (8)$$

where B'_n is obtained from B_n by exchanging all the $\vec{a}_k$ and $\vec{a}'_k$. The maximal value allowed by QM is $S_M = 2^{\frac{M+1}{2}}$, achieved for M-qubit GHZ states. An important property of these inequalities is the following: the bound $S_M \leq 2^{\frac{m+1}{2}}$, with $m < M$, can be violated only by states in which more than m qubits are entangled [22,23]. We shall say that a M-qubit state violates the inequality if for this state $S_M > 2^{\frac{M}{2}}$, that is, if the violation can be accounted for only by having M-qubit entanglement.

Having settled these notions, we can prove

Theorem 2: *The state $|\Psi_{Nh}\rangle$ given in (7) is such that the authorized partners violate the N-qubit MK inequality (in the sense just described) if and only if $\phi < \frac{\pi}{4}$; and in this range, the unauthorized partners do not violate the $(N-h+1)$-qubit MK inequality. At $\phi = \frac{\pi}{4}$, both sets of partners are exactly at the border of the violation; and for $\phi > \frac{\pi}{4}$ the roles of the authorized and the unauthorized partners is reversed.*

The proof (see [12] for all details) is a direct optimization of expressions like $\langle\Psi_{Nh}|B_N(\underline{a}) \otimes \mathbb{1}|\Psi_{Nh}\rangle$ over all sets of $2N$ unit vectors $\underline{a}$. This optimization is not easy. We could perform it analytically when N and h have different parities (in particular, this is the case if $h = N-1$, that is when all partners are honest and Eve is external); and some cases where N and h have the same parity were checked on the computer. Therefore, to within the limitations of this proof, we can safely say that: for the N-QSS protocols, and whatever the eavesdropping scenario in which Eve uses the best individual attack, the security condition $I_a > I_u$ is satisfied if and only if the authorized partners violate the MK inequality, and in this case the unauthorized partners do not violate the MK inequality. We recall that "violation" here does not merely mean

$S_M > 2$, the limit imposed by lhv, but $S_M > 2^{\frac{M}{2}}$, i.e. that all the qubits are really strongly entangled.

One might ask if a purely algebraic result like Theorem 1 holds for the violation of any M-qubit MK inequality. The answer is negative. As a counterexample, the four-qubit state $\cos\alpha(|0011\rangle + |1100\rangle + i|0101\rangle + i|1010\rangle)/2 + \sin\alpha(i|1001\rangle + |1111\rangle)/\sqrt{2}$ gives $S_{ABC} = S_{BCD} = 3 > 2\sqrt{2}$ for $\alpha \approx 0.955$. However, we have numerical evidence that no such states can be produced by Eve. Our current knowledge on this question can be found in [12]. In any case, the fact that a general algebraic theorem does not hold in all cases *strengthens* the link between security and violation of a MK inequality: even though in the Hilbert space we can find states that violate two inequalities for some shared qubits, these states do not appear in the individual eavesdropping on a N-QSS protocol.

This leads us naturally to the question of the choice of the optimal Bell's inequalities. Our choice of the MK inequalities is natural in the following sense: we are considering QKD protocols in which each partner measures two conjugated observables; therefore, we choose also inequalities with two measurements per qubit. Werner and Wolf have recently classified all the inequalities of this class, and have demonstrated that the MK inequalities are those that give the highest violation, for GHZ states [24]. It is not impossible that other inequalities may be better suited for the study of security in other protocols with more than two settings per qubit. For instance, in the six-state QKD between two partners it is known that $S_{AB} > 2 > S_{AE}$ is a sufficient but not a necessary condition for security [3,25].

Of course, we share the open questions of the whole field of quantum cryptography: which is Eve's best attack in all generality? Or, does something change if the partners share higher dimensional systems instead of qubits? Note also that no satisfactory Bell's inequality has been found yet for higher dimensional systems. Under these respects, the study of the link between Bell's inequalities and security seems to be a promising field of research, at the border between quantum information and foundations of quantum mechanics.

We conclude by stressing that Bell's inequalities appear here in a context that is disconnected (at least at first sight) from the studies on lhv: we have only discussed entanglement — to be precise, an entanglement that is "useful" for some quantum communication protocols. In other words, Bell's inequalities seem to have a role to play in "present-day" quantum information processing, and not only in the "old" debate on lhv.

[1] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics: Collected papers on quantum philosophy* (Cambridge University Press, Cambridge, 1987).

[2] D. Bouwmeester, A. Ekert and A. Zeilinger (eds.), *The Physics of Quantum Information* (Springer, Berlin, 2000).

[3] For a recent review article, see: N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, e-print quant-ph/0101098 (2001); to appear in Rev. Mod. Phys.

[4] B. Huttner, N. Gisin, *Phys. Lett. A* **228** (1997) 13

[5] C. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, A. Peres, *Phys. Rev. A* **56** (1997) 1163

[6] A. Ekert, *Phys. Rev. Lett.* **67** (1991) 661

[7] C. Bennett, G. Brassard, in: *Proceedings of the Int. Conf. on Computer, System and Signal Processing, Bangalore, India* (IEEE, New York, 1984); C. Bennett, G. Brassard, N.D. Mermin, *Phys. Rev. Lett.* **68** (1992) 557.

[8] I. Csiszár, J. Körner, *IEEE Trans. Inf. Theory* **IT-24** (1978) 339

[9] N. Gisin, S. Wolf, *Phys. Rev. Lett.* **83** (1999) 4200

[10] P.W. Shor and J. Preskill, *Phys. Rev. Lett.* **85** (2000) 441, and ref. therein.

[11] C.-S. Niu, R.B. Griffiths, *Phys. Rev. A* **60** (1999) 2764

[12] V. Scarani, N. Gisin, e-print quant-ph/0104016

[13] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, *Phys. Rev. Lett.* **23** (1969) 880

[14] B.S. Cirel'son, *Lett. Math. Phys.* **4** (1980) 83

[15] I. Pitowski, *Quantum probability, quantum logic*, Lecture Notes in Physics 321 (Springer, Heidelberg, 1989)

[16] M. Horodecki, P. Horodecki, M. Horodecki, *Phys. Lett. A* **200** (1995) 340

[17] Writing $\vec{a}_+ = \vec{a}$, $\vec{a}_- = \vec{a}\,'$, $\vec{A}_+ = \vec{A}$ and $\vec{A}_- = \vec{A}\,'$, the full expression for f is

$$f = \left|\vec{a} \wedge \vec{a}\,'\right|^2 \left|\vec{b} \wedge \vec{b}\,'\right|^2 + \left|\vec{A} \wedge \vec{A}\,'\right|^2 \left|\vec{c} \wedge \vec{c}\,'\right|^2 +$$
$$+ \sum_{\sigma,\omega=\pm} (\vec{a}_\sigma \cdot \vec{A}_\omega)^2 (1 + \sigma\vec{b} \cdot \vec{b}\,')(1 + \omega\vec{c} \cdot \vec{c}\,')\,.$$

[18] N. Gisin, *Phys. Lett. A* **210** (1996) 151

[19] The same behavior is shown by the states introduced in [4], where it was erroneously claimed that both pairs Alice-Bob1 and Alice-Bob2 violate the CHSH inequality.

[20] We use the name *quantum secret sharing* in its original meaning (the distribution of secret classical bits using quantum channels), as in: A. Karlsson, M. Koashi, and N. Imoto. *Phys. Rev. A* **59** (1999) 162; M. Hillery, V. Buzek, and A. Berthiaume, *Phys. Rev. A* **59** (1999) 1829; W. Tittel, H. Zbinden, N. Gisin, *Phys. Rev. A* **63** (2001) 042301. Later, the same name was also used for the "sharing of a quantum secret (state)": R. Cleve, D. Gottesman, H.-K. Lo, *Phys. Rev. Lett.* **83** (1999) 648.

[21] N.D. Mermin, *Phys. Rev. Lett.* **65** (1990) 1838; A.V. Belinskii, D.N. Klyshko, *Phys. Usp.* **36** (1993) 653

[22] N. Gisin, H. Bechmann-Pasquinucci, *Phys. Lett. A* **246** (1998) 1

[23] R.F. Werner, M.M. Wolf, *Phys. Rev. A* **61** (2000) 062102

[24] R.F. Werner, M.M. Wolf, e-print quant-ph/0102024 (2001). To appear in Phys. Rev. A

[25] D. Bruss, *Phys. Rev. Lett.* **81** (1998) 3018; H. Bechmann-Pasquinucci, N. Gisin, *Phys. Rev. A* **59** (1999) 4238